IN THE CLAIMS

The claim set is intended to reflect amendment of previously pending claims 1, 10, 18, 28, and 34, and addition of new claims 38-42. The specific amendments to individual claims are detailed in the following marked up set of claims.

1. (Currently Amended) A security modeling system comprising:

a network configuration module having network configuration data; ~~and~~

a simulator coupled to the network configuration module ~~for simulating and analyzing~~ to simulate and analyze networks based on the network configuration data, wherein the simulator includes a network vulnerabilities database, and wherein the network vulnerabilities database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

2. (Original) The system of claim 1, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

3. (Original) The system of claim 2, wherein the network configuration data and the network vulnerability, attack and exploitation data are stored in database tables and the data is processable by a computer.

4. (Original) The system of claim 1, wherein the network configuration module comprises network configuration data output by a network configuration discovery tool.

5. (Original) The system of claim 1, wherein the simulator includes a graphical user interface.

6. (Original) The system of claim 2, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

7. (Original) The system of claim 1, wherein the simulator includes a defender and an attacker user interface.

8. (Original) The system of claim 1, wherein the security modeling system is portable.

9. (Original) A computer game comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game.

10. (Currently Amended) A security modeling system comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database; and

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

11. (Original) The system of claim 10, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

12. (Original) The system of claim 11, wherein the network configuration data and the network vulnerability, attack and exploitation data is stored in database tables and the data is processable by a computer.

13. (Original) The system of claim 10, wherein the simulator includes a graphical user interface.

14. (Original) The system of claim 10, wherein the critical resource information includes goals, expectations and constraints for simulating the network.

15. (Original) The system of claim 10, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

16. (Original) The system of claim 10, wherein the security modeling system is portable.

17. (Original) The system of claim 10, wherein the simulator includes a defender and an attacker interface.

18. (Currently Amended) A method of analyzing a computer network using a security modeling system, wherein the security modeling system includes a database of network vulnerability information, the method comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

19. (Original) The method of claim 18, wherein providing a network configuration includes receiving a configuration as the output of a network discovery tool.

20. (Original) The method of claim 18, wherein providing a network configuration includes receiving a data file which includes a configuration of the computer network.

21. (Original) The method of claim 18, wherein simulating the network includes:
receiving mission objectives;
storing the objectives; and
simulating the network based on the network configuration and mission objectives.

22. (Original) The method of claim 21, wherein determining vulnerabilities includes modifying the simulation using a graphical user interface.

23. (Original) The method of claim 22, wherein modifying the simulation includes dynamically interacting with an attacker.

24. (Original) The method of claim 22, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

25. (Original) The method of claim 23, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

26. (Original) The method of claim 21, wherein determining vulnerabilities includes computing security results, wherein the security results include a security score.

27. (Original) The method of claim 21, wherein determining vulnerabilities of the simulated network includes updating the vulnerabilities database when vulnerabilities are detected.

28. (Currently Amended) A method of opposing network attackers comprising:

receiving a network configuration, wherein the network configuration comprises computer hardware and software component information;

receiving mission objectives including critical resource information used to determine network components that are involved in a specific attack scenario;

receiving commands from a network attacker;

simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components; and

responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network.

29. (Original) The method of claim 28, wherein simulating the network further includes receiving commands from a defender and determining results based on the defender commands.

30. (Original) The method of claim 28, wherein receiving configuration includes receiving critical resource information, wherein the critical resource information includes goals, expectation and constraints for simulating the network.

31. (Original) The method of claim 28, and further includes modifying the simulation using a graphical user interface.

32. (Original) The method of claim 31, wherein determining vulnerabilities includes computing security results which include a security score.

33. (Original) The method of claim 31, wherein receiving commands includes receiving attack actions which include commands that simulate service functionality, commands that change services or nodes, and commands that exploit vulnerabilities.

34. (Currently Amended) A security modeling system for simulating objective networks comprising:

a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables including information used to determine network components that are involved in a specific attack scenario, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data; and

a graphical user interface which operates with the simulator to allow input and output to clients.

35. (Original) The system of claim 34, wherein the mission objectives tables include mission tables, mission files tables and mission services tables.

36. (Original) The system of claim 34, wherein the vulnerability tables include service tables.

37. (Original) The system of claim 34, wherein the network configuration tables include configuration tables, defense tables, filter tables, node tables, routing tables and password tables.

38. (New) The computer game of claim 9, wherein the simulator further comprises:

an attacker interface to transmit real-time network status information to an attacker during a simulation; and

a defender interface to transmit real-time network status information to a defender during a simulation.

39. (New) The computer game of claim 9 further comprising:

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

40. (New) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes the service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

41. (New) The machine-readable medium of claim 40, wherein simulating the network includes:

receiving mission objectives;

storing the objectives; and

simulating the network based on the network configuration and mission objectives.

42. (New) The machine-readable medium of claim 41, wherein mission objectives include critical resource information used to determine network components that are involved in a specific attack scenario.